IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 11, 2006

(Date of Deposit)

James D. Wood
Name of person mailing Document or Fee

Signature

January 11, 2006
Date of Signature

Re: Application of: Waters et al.
Serial No.: 09/827,291
Filed: April 5, 2001
For: System and Method for Implementing Financial Transactions Using Biometric Keyed Data
Group Art Unit: 3621
Confirmation No. 5721
Examiner: Kambiz Abdi
MMB Docket No.: 1001-0724
NCR Docket No. 9385

TRANSMITTAL OF APPEAL BRIEF

Please find for filing in connection with the above patent application the following documents:

1. Appeal Brief (32 pages);

2. A Check in the amount of $500.00; and

3. One (1) return post card.

Please charge any fee deficiency or credit any overpayment to Deposit Account No. 13-0014.

Respectfully Submitted,

MAGINOT, MOORE & BECK

January 11, 2006

James D. Wood
Registration No. 43,285
Chase Tower
111 Monument Circle, Suite 3250
Indianapolis, IN 46204-5109

Enclosures

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

NCR Docket No. **9385**

MMB Docket No. **1001-0724**   Confirmation No.: **5721**

Application of: **Waters et al.**   Group Art Unit: **3621**

Serial No.: **09/827,291**   Examiner: **Kambiz Abdi**

Filed: **April 5, 2001**

For: **SYSTEM AND METHOD FOR IMPLEMENTING FINANCIAL**
TRANSACTIONS USING BIOMETRIC KEYED DATA

01/17/2006 BABRAHA1 00000001 09827291
01 FC:1402   500.00 OP

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 11, 2006
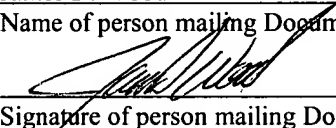(Date of Deposit)

James D. Wood
Name of person mailing Document or Fee

Signature of person mailing Document or Fee

January 11, 2006
Date of Signature

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal under 37 CFR § 1.191 to the Board of Patent Appeals and

Interferences of the United States Patent and Trademark Office from the final rejection of

the claims 1-4, 6-11 and 13-17 of the above-identified patent application. These claims were indicated as finally rejected in a Final Office Action dated November 16, 2005. The $500.00 fee required under 37 CFR § 41.20(b)(2) is included herewith. Also, please provide any extensions of time that may be necessary and charge any fees that may be due to Account No. 13-0014, but not to include any payment of issue fees.

(1) REAL PARTY IN INTEREST

NCR Corporation of Dayton, Ohio is the assignee of this patent application, and the real party in interest.

(2) RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences related to this patent application (serial no. 09/827,291).

(3) STATUS OF CLAIMS

Claims 1-4, 6-11 and 13-17 are pending in the application.

Claims 5 and 12 have been canceled.

Claims 1-4, 6-11 and 13-17 are finally rejected.

Claims 1-4, 6-11 and 13-17 are being appealed, and are shown in the Appendix attached to this Appeal Brief.

(4) STATUS OF AMENDMENTS

Appellants have filed no amendments after receipt of the November 16, 2005,

Final Office Action (the "Office Action").

(5) SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to a method of implementing financial transactions using biometric data. (Appellants' specification at page 1, lines 4-6). In one embodiment, a system 10 includes a biometric input device 14, a payment device 18, a merchant payment host 20 and an identity lookup database 24. (Appellants' specification at page 7, lines 11-14 and FIG. 1).

The data records in the database 24 are organized for retrieval by data storage keys, in a relational database, or object identifiers, in an object repository. (Appellants' specification at page 8, lines 8-10). The storage keys/identifiers correspond to the biometric data of the customer. (Appellants' specification at page 8, lines 8-10). For example, when a financial account is established, a biometric data capture device is used to capture biometric data from the consumer. (Appellants' specification at page 8, lines 12-14 and FIG. 2A). The biometric data may then be input to a hashing function or the like to generate the data storage key. (Appellants' specification at page 8, lines 14-16). The key in this type of embodiment represents a statistically unique key for the individual. (Appellants' specification at page 8, line 21 through page 9, line 1). Alternatively, another key may be generated using additional data, such as the name of the customer, to be used in conjunction with the key from the biometric data to uniquely identify a record. (Appellants' specification at page 9, lines 7-16).

In an exemplary operation, a customer who is registered in the system cooperates with a biometric device so that the system can obtain biometric data from the customer at

a transaction site. (Appellants' specification at page 10, lines 2-4 and FIG. 2B block 120). The biometric data is sent to the merchant host 20 which uses the biometric data to generate a data storage key. (Appellants' specification at page 10, lines 4-8 and FIG. 2B blocks 124-128). The database 24 is then searched for a financial account identified with an identical key. (Appellants' specification at page 10, lines 8-10 and FIG. 2B block 130). If a financial account data record is identified (i.e. the record is identified by a key that is identical to the key generated using the biometric data from the transaction site), then the data record is retrieved. (Appellants' specification at page 10, lines 10-12 and FIG. 2B block 136).

After the financial account data record has been retrieved, the biometric data obtained at block 120 may further be used by the merchant host 20 to verify that the biometric key was used to retrieve the correct by comparing the biometric data obtained at block 120 with biometric data from the retrieved financial record that was stored in the financial record at the time the customer registered for the account. (Appellants' specification at page 10, lines 13-16 and FIG. 2B block 144). After comparison of the biometric data, an account message is generated and transmitted to the transaction site to allow completion of the transaction. (Appellants' specification at page 10, line 13 through page 11 line 19 and FIG. 2B blocks 150-198).

Accordingly, the present invention uses biometric data to generate a unique identifier or data storage key for a financial account record. The biometric data may also be stored in the financial account record. A biometric key generated from biometric data obtained at the time of a transaction is used thereafter to retrieve the uniquely identified financial account record. After the financial account record is retrieved, the obtained

4

biometric data may further be used to verify that the retrieved record is the correct record by comparing the biometric data obtained at the transaction site with the stored biometric data.

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-4, 6-11 and 13-17 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,662,166 B2 to Pare, Jr. et al. (hereinafter "Pare") in view of U.S. Patent No. 6,202,151 B1 to Musgrave et al. (hereinafter "Musgrave").

(7) ARGUMENT

Claims 1, 2, 8-11 and 15 Are Not Obvious

Discussion Regarding Claim 1

Claim 1 stands rejected under 35 U.S.C. §103(a) as being obvious over Pare in view of Musgrave. (Office Action at page 5). Pare is not available as prior art. Moreover, there is no motivation for the proposed combination and the proposed modification fails to arrive at the invention of claim 1 when claim 1 is properly construed. Accordingly, the rejection of claim 1 should be reversed.

1. Claim 1

Claim 1 states:

> A system for providing consumer access to a financial account to implement a transaction comprising:
> a biometric data capture device for reading consumer biometric data; and
> a database server for generating a data storage key from the consumer biometric data received from the biometric data capture device and for retrieving a financial account data record corresponding to the generated data storage key.

Claim 1 thus recites a system wherein the financial account of an individual is identified by a key that is generated using biometric data of the individual.

2.   Pare is Not Proper Prior Art

The Examiner has relied primarily upon Pare as disclosing the elements recited in claim 1 with further reference to Musgrave solely for teaching a method for generating a digital signal with a concatenator using biometric data. (Office Action at page 5). Because Pare is not available as prior art, the Examiner has failed to present a *prima facie* case of obviousness.

When a patent is used as a reference, the MPEP states that "[t]he filing date, in most instances also given on the face of the patent, is ordinarily the effective date as a reference." MPEP § 901.04. The filing date for Pare is June 11, 2001. The Appellants' application was filed on April 5, 2001. Accordingly, the filing date of the Appellants' application precedes the effective date of Pare as a reference.

Therefore, because the Examiner has failed to allege that reliance on Pare is proper under the exception to the rule that the critical reference date must precede the filing date as set forth in MPEP § 2124, Pare is not available as a reference under 35 U.S.C. 103 for the Appellants' application. Thus, because the Examiner has failed to identify all of the elements recited in claim 1 in an effective reference, the Examiner has

failed to present a *prima facie* case of obviousness and the Board of Appeals is

respectfully requested to reverse the rejection of claim 1.[1]

3. There is No Motivation for the Proposed Combination

The Examiner admits that Pare fails to disclose each element of claim 1 but

alleges that the missing element is provided by Musgrave. (Office Action at page 5).

Because there is no motivation for the proposed modification of Pare, the Examiner has

failed to present a *prima facie* case of obviousness.

Specifically, the Examiner alleges that the motivation to modify Pare to allegedly

arrive at the invention of claim 1, is the desire for "enhancement of security as well as

accuracy as well as reduction of computational resources." (Office Action at page 6). The

Federal Circuit has stated, however, that "[the] factual question of motivation is material

to patentability, and [cannot] be resolved on subjective belief and unknown authority. It

is improper, in determining whether a person of ordinary skill would have been led to this

combination of references, simply to '[use] that which the inventor taught against its

teacher.'" *In re Lee*, 277 F.3d 1338, 1343-1344 (Fed. Cir. 2002)(internal citations

omitted). Significantly, the Federal Circuit in *In re Lee* determined that an examiner's

conclusory statements that "the demonstration mode is just a programmable feature

which can be used in many different device[s] for providing automatic introduction by

adding the proper programming software" and that "another motivation would be that the

---

[1] The Appellants previously brought the effective date of Pare to the attention of the Examiner. (See Appellants' Response dated August 23, 2005). In response, the Examiner tasked the Appellants with determining which parts of Pare were not supported by an earlier date. (Office Action at page 2). The Appellants are not aware of any legal basis for the unstated theory that an unavailable reference may be relied upon to make a *prima facie* case of obviousness unless an applicant affirmatively proves that the disclosure relied upon is *not* supported by an effective reference.

automatic demonstration mode is user friendly and it functions as a tutorial" did not adequately address the issue of motivation to combine. (Id. at 1343).

Likewise, the Examiner has made conclusory statements regarding the motivation to combine the references. Specifically, "enhancement of security as well as accuracy as well as reduction of computational resources" may well be sufficient *benefits* to support a *prima facie* case of obviousness when these benefits are *only* associated with the piece of art proposed to be used in modifying a primary reference. That is not the situation with respect to the systems of Pare and Musgrave.

As an initial matter, Pare, the primary reference, purports to provide security and accuracy as it "virtually eliminates the risk of denying access to rightful users while simultaneously protecting against granting access to unauthorized users." (Pare at column 6, lines 58-60). Moreover, Pare purports to achieve these benefits while "reducing the cost of equipment and staff required to collect, account, and process [credit] transactions." (Pare at column 6, lines 23-25). The Examiner has failed to allege, much less show, that Pare fails in providing the claimed benefits, thereby necessitating the incorporation of the teaching of Musgrave to achieve those benefits.

Additionally, the Pare inventors were aware of the teaching of Musgrave. The listing of references cited for Pare shows that the Pare inventors cited Musgrave to the examiner. Therefore, since Pare specifically incorporated the teachings of a number of patents (see, e.g. Pare at column 2, line 64 through column 3, line 10) but chose not to incorporate the teachings of Musgrave when the teachings of Musgrave were obviously known, it is apparent that the Pare inventors believed that the means by which the system of Pare achieved the recited benefits was preferred over the incorporation of the system

8

of Musgrave. As the Federal Circuit has stated, "[t]he mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination." *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Clearly, the inventors of Pare did not identify any desirability for the proposed modification. Likewise, the Examiner has failed to identify any desirability for the proposed modification by showing how Pare fails to meet its stated objectives or how Musgrave would provide any additional benefit.

Moreover, the Examiner has failed to identify any teaching, disclosure or suggestion that the system of Musgrave provides, in general, the alleged benefits. The sole attempt by the Examiner to find support for his characterization of Musgrave is a citation to Musgrave at column 3, lines 8-22. (Office Action at page 6). In the cited passage, Musgrave merely identifies a *problem* in the prior art. Namely, that "the relatively large computational demands of authentication techniques based upon physical characteristics has prevented such authentication techniques from being implemented in electronic transactions." (Musgrave at column 3, lines 19-22). It is possible that the system of Musgrave overcomes the shortcomings of the prior art, however, the Examiner has failed to make any such allegation and it is not the responsibility of the Appellants to present a *prima facie* case. Moreover, the cited passage merely speaks to computational resources, not to accuracy or security.

Therefore, the Examiner has failed to make any showing that the benefits of improved accuracy, security and reduced computational resources would be realized by replacing some unidentified portion of the system of Pare with the concatenator from the system of Musgrave. Thus, the Examiner has failed to identify either a sufficient basis or

a proper source for the proposed motivation to combine the teachings of Pare with the teachings of Musgrave. Accordingly, under MPEP § 2143.01, the Examiner has failed to present a *prima facie* case of obviousness and the rejection of claim 1 under 35 U.S.C. 103(a) should be reversed.

4. Claim 1 Has Been Misconstrued

The Examiner has explained the basis for his construction of claim 1 in the Office Action at pages 3-4. As evidenced therein, the Examiner has misconstrued claim 1. It is the retrieval of the financial record in the first instance that is recited in the claim and it is this limitation that the Examiner has ignored in determining that the elements of claim 1 are disclosed in Pare '166. When properly construed, claim 1 recites elements not present in the prior art.

a. The Examiner's Construction.

Claim 1 recites a "database server for generating a data storage key from the consumer biometric data and for retrieving a financial account data record corresponding to the generated data storage key." While it is proper to give a claim element its broadest reasonable construction in examination proceedings, the Examiner has attempted to generalize this element to the extent that explicit limitations in the element are no longer a part of the claim while limitations not found in the claim are imported from the Appellants' specification.

Specifically, the Examiner initiates the explanation of his construction by first generalizing the claim limitations with the characterization that "[t]he claims state clearly

that a biometric data is captured and based on the biometric data a financial account is identified for transaction (sic)." (Office Action at page 3). While this characterization is not *per se* incorrect, it fails to retain the recited limitation dealing with "storage keys" as discussed below.

The Examiner then imports a limitation from the Appellants' specification into the claim by opining that "[t]he captured biometric information is essentially used for authentication." (Office Action at page 3). In support of this sleight-of-hand, the Examiner alleges that the summary of the invention (paragraph 9 of the Appellants' specification) "clearly states that 'retrieving a data record corresponding to a consumer and retrieving a data record corresponding to the data storage key and the record contains customer financial data.'" (Office Action at page 3).

Thus, the Examiner has read the limitation that the data storage key is generated from the biometric data out of the claim, and then read into the claim a limitation that the biometric data is used for verification of the identity of the person attempting to access a financial record.

Based upon the foregoing explanation, the Examiner construes the claimed method to recite steps wherein "there is and (sic) identification and authentication of the person providing the biometric information and then if there is (sic) no discrepancies and the biometric data match with stored biometric data in the database, then the identification of the financial account takes place as it has been clearly disclosed by the Pare '166 as it has been presented in the rejection below." (Office Action at page 4). This construction effectively eliminates the limitation of a data storage key generated

from biometric data and replaces it with a limitation of "using biometric data to authenticate the identity of a customer."

b. The Word "Key" is a Key Word

The Applicants agree that Pare '166 teaches the use of stored biometric data to authenticate a person submitting the biometric data and that thereafter a financial record identified in the person's record is obtained. The Applicants' specification also teaches that biometric data is used to authenticate that the proper financial record has been retrieved. (Appellants' specification at page 10, lines 14-17 and FIG. 2B, block 144). Under a proper construction of claim 1, however, Pare fails to disclose a database server as recited in claim 1.

It is well established that the words of a claim must be given their plain meaning unless an applicant has provided a clear alternate definition in the specification. *In re Zletz*, 893 F.2d 319, 321, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989). Claim 1 clearly recites that the database server is for "generating a data storage key from the consumer biometric data." *The Free On-line Dictionary of Computing*, http://www.foldoc.org/, Ed. Denis Howe, 1993-2005 defines a "key" in the following manner:

> A value used to identify a record in a database, derived by applying some fixed function to the record. The key is often simply one of the fields (a column if the database is considered as a table with records being rows, see "key field"). Alternatively the key may be obtained by applying some function, e.g. a hash function, to one or more of the fields. The set of keys for all records forms an index. Multiple indexes may be built for one database depending on how it is to be searched.

Therefore, there is a distinction between values which form an index used to search for and retrieve records and values stored within the record that may be used after

retrieval of the record for authentication. Accordingly, a "key" is a value that uniquely *identifies* a particular record so as to allow retrieval of the record. Thus, the generation of "a data storage key from the consumer biometric data" as recited in claim 1 means that the biometric data is used to generate a value that uniquely identifies a data storage record so that the data storage record may be retrieved. The claim further recites that the data storage record is "a financial account data record." Therefore, the plain meaning of the words in the claim is that the database server uses biometric data to generate a value which uniquely identifies a particular financial data record so that the financial data record may be retrieved.

Consequently, the Examiner's construction, whereby the biometric data only authenticates an individual but does not uniquely identify a financial record, is contrary to the plain meaning of the words in the claim.

c. The Specification Supports the Plain Meaning of "Key"

Of course, the plain meaning of the words must be determined in the context of the application. As stated by the Federal Circuit, "claims are not to be read in a vacuum, and limitations therein are to be interpreted in light of the specification in giving them their 'broadest <u>reasonable</u> interpretation'." *In re Marosi,* 710 F.2d 799, 802, 218 USPQ 289, 292 (Fed. Cir. 1983), <u>quoting</u> *In re Okuzawa,* 537 F.2d 545, 548, 190 USPQ 464, 466 (CCPA 1976)) (emphasis in original).

The definition of "key" set forth above comports with the use of the word in the specification. By way of example, at page 8, lines 8-10, the Appellants' specification states "[t]he data records of database 24 are organized for retrieval by data storage keys,

in a relational database, or object identifiers, in an object repository, that correspond to the biometric data for the consumer.

Therefore, the specification supports the plain meaning of the words in the claim.

d. The Examiner Misquoted the Specification

Obviously, the portion of the specification allegedly quoted by the Examiner appears to introduce some level of ambiguity in the construction of claim 1 as it contradicts both the plain meaning of the claim as discussed above as well as the above quotation from page 8 of the Appellants' specification. The ambiguity results, however, from a misrepresentation of the Appellants' specification by the Examiner rather than from any disclosure within the specification.

The portion of the Appellants' specification which the Examiner purports to have quoted actually states "the present invention includes generating a data storage key from a set of biometric data corresponding to a consumer and retrieving a data record corresponding to the data storage key and the record contains customer financial account data." (Appellants' specification at paragraph 9). In other words, the biometric data of a consumer is used to generate a data storage key and the data storage key corresponds to a financial record.

Therefore, when read properly, the portion of the Appellants' specification relied upon by the Examiner supports the plain meaning of the claim and *not* the Examiner's construction.

e. Conclusion

The claim clearly recites a database server which uses biometric data to generate a value (key) which uniquely identifies a particular financial storage record, and which retrieves the financial record using that unique value (key). Appellants' specification does disclose the use of biometric data in authenticating a retrieved file. Significantly, this disclosure is found in a description of the *preferred embodiment*, not in the summary of the invention as alleged by the Examiner. Moreover, the Appellants' specification consistently discloses that the authentication step is *after* the record has been *retrieved*.

The Examiner has failed to identify any valid basis for reading the biometric key limitation out of claim 1 such that "there is no indication of direct retrieval of the financial information from the biometric information" and replacing the element with an authentication limitation so as to read upon the system of Pare. (See Office Action at page 4). Therefore, the Examiner's construction of claim 1 is unreasonable and the Board of Appeals is respectfully requested to overturn the rejection of claim 1 because the Examiner's rejection rests upon a flawed construction of the claim.

5.   Modification of Pare Does Not Arrive at the Invention of Claim 1

The Examiner has also stated, however, that the system of Pare discloses "a database server for generating a data storage key from the consumer biometric data received from the biometric data capture device and for retrieving a financial record corresponding to the generated data storage key." This appears to be mere parroting of the Appellants' claim language with the intent that it be construed in the manner suggested by the Examiner as discussed above. Nonetheless, in the event that the

15

Examiner actually intended to allege that Pare disclosed the type of database server recited in claim 1, the Examiner has mischaracterized Pare.

Specifically, the Examiner has alleged that Pare discloses a database server wherein the financial account of an individual is identified by a key that is generated based upon biometric data of the individual at "figure 2 and 3 and associated text, column 4, lines 34-37, column 5, lines 15-55, column 6, lines 67-13 (sic) and lines 47-54, and column 9, lines 54-58." (Office Action at page 3). A review of Pare, however, reveals that the Examiner has erroneously equated "verifying the identity of an individual" with "identifying a financial account."

For example, FIG. 2 shows a "party identifying apparatus" (PIA). As described at column 7 line 54 through column 8 line 63 of Pare, the PIA 1 is merely a sensor device for obtaining biometric data. There is no discussion of using any biometric data obtained with the PIA to generate a key used to obtain a financial account record. Rather, the device is used merely to provide biometric data which is used by an identification module to identify the individual attempting to complete a transaction. (Pare at column 10, lines 3-5). Fig. 3, as described at column 9, lines 44-47 of Pare, modifies the system of FIG. 2 by including the use of a cellular digital packet data. Accordingly, FIGs. 2 and 3 of Pare do not disclose a database server as recited in claim 1.

At column 4, lines 34-37, Pare merely states that an object of the invention is to eliminate the use of personal identification numbers in accessing a financial account. A stated objective is not a disclosure of a particular manner in which to accomplish the objective. Accordingly, this citation of Pare does not support the rejection of claim 1.

16

At column 5, lines 15-55, Pare clearly states that the invention disclosed therein "identifies the payor" and that thereafter financial account data is retrieved. (Pare at column 5, lines 18-19). A payor is not a financial account record and this passage fails to identify any mechanism that is used to retrieve the financial account data. Accordingly, this section of Pare does not disclose retrieving a financial account data record using a key generated from biometric data.

At column 6, lines 7-13 and lines 47-54, Pare discloses that an object of the invention is to provide a person with simultaneous direct access to financial accounts. A stated objective is not a disclosure of a particular manner in which to accomplish the objective. Accordingly, this section of Pare does not support the rejection of claim 1.

At column 9, lines 54-58, Pare discloses that the data processing centers retrieve financial account information "for identified parties." Once again, however, there is no disclosure of how the retrieval of the financial documents is effected, only that such retrieval occurs after the biometric data is used to identify the individual.

Accordingly, Pare clearly discloses the use of biometric data to identify an individual by comparing received biometric data with biometric data stored in a record. Pare fails, however, to disclose using a key generated from the biometric data to *retrieve* a financial account data record. Comparing data found in a file with received data is not the same as retrieving the file using the received data. Therefore, even if Pare is modified to include the use of Musgrave's concatenator, the modification does not arrive at invention of claim 1. Thus, under MPEP § 2143.03, the Examiner has failed to present a *prima facie* case of obviousness and the rejection of claim 1 under 35 U.S.C. 103(a) should be reversed.

6.   Conclusion

For any or all of the foregoing reasons, it is respectfully submitted that the rejection of claim 1 as being obvious over Pare in view of Musgrave is in error and the Applicants respectfully request the Board of Appeals to reverse the rejection of claim 1 under 35 U.S.C. § 103.

Discussion Regarding Claim 2

Claim 2 depends from claim 1 and incorporates all of the limitations of claim 1. Therefore, for at least any of the same reasons set forth above with respect to the rejection of claim 1, the rejection of claim 2 is in error and the Board of Appeals is respectfully requested to reverse the rejection of claim 2.

Discussion Regarding Claims 8-11 and 13-15

Claims 8, 13 and 15 are independent claims. Each of these claims recites limitations analogous to limitations of claim 1 which, for purposes of this appeal, result in a method using a key generated from biometric data to retrieve a financial account data record. Claims 9-11 depend from claim 8 and incorporate all of the limitations of claim 8 and claim 14 depends from claim 13 and incorporates all of the limitations of claim 13. Therefore, for at least any of the same reasons set forth above with respect to the rejection of claim 1, the rejection of claims 8-11 and 13-15 is in error and the Board of Appeals is respectfully requested to reverse the rejections of claims 8-11 and 13-15.

Claims 3 and 4 Are Not Obvious

Discussion Regarding Claim 3

Claim 3 stands rejected under 35 U.S.C. §103(a) as being obvious over Pare in view of Musgrave. (Office Action at pages 5 and 6). The proposed modification fails to arrive at the invention of claim 3. Moreover, there is no motivation for the proposed combination. Accordingly, the rejection of claim 3 should be reversed.

1.   Claim 3

Claim 3 states:

> A system for supporting consumer access to a financial account by means of biometric data solely, the system comprising:
>   a biometric data capture device for capturing biometric data corresponding to a consumer; and
>   a payment device for sending said captured biometric data to a merchant payment host as the identifier for the consumer's financial account data.

Claim 3 thus recites a method which *solely* uses captured biometric data to identify a consumer's financial account data.

2.   The Discussion of Claim 1 Applies to Claim 3

The Examiner rejected claim 3 based upon the same reasoning set forth above with respect to the rejection of claim 1. (Office Action at page 5). For the purposes of this appeal, the limitation in claim 3 that the biometric data is used as the identifier, in an object repository, for the consumer's financial account data is the same as the data storage key, in a relational database, discussed above with respect to claim 1. Therefore, the discussion of claim 1 applies to claim 3 and the Board of Appeals is respectfully requested to reverse this rejection of claim 3.

19

3.   The Examiner has Misconstrued the Claim

Additionally, the Examiner has stated that "there is no indication of direct retrieval of the financial information from the biometric information." (Office Action at page 3). While this statement may only be directed to a discussion of an embodiment that was disclosed in the Appellants' specification, it is more likely that the Examiner was attempting to argue that the claims were not expressly limited to only using biometric data for the retrieval of financial information. (See, e.g., Office Action at pages 3-4). The Examiner has misconstrued the claim.

Specifically, the preamble of claim 3 recites "[a] system for supporting consumer access to a financial account by means of biometric data solely." The Federal Circuit has stated that "[i]f the claim preamble, when read in the context of the entire claim, recites limitations of the claim, or, if the claim preamble is 'necessary to give life, meaning, and vitality' to the claim, then the claim preamble should be construed as if in the balance of the claim." *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305, 51 USPQ2d 1161, 1165-66 (Fed. Cir. 1999).

The word "solely" is defined as "entirely; exclusively." *The American Heritage® Dictionary of the English Language*, Fourth Edition, Copyright 2000. Therefore, the claim preamble identifies a direct correspondence between the "identifier" for the financial account and the captured biometric data. In other words, the identifier for the financial account includes nothing more than the obtained biometric data. Thus, the use of the word "solely" in the preamble of claim 3 limits the scope of the "identifier" to

being generated from the captured biometric data. Accordingly, the preamble is a limit on the claim and must be construed as if it is in the balance of the claim.

Therefore, and contrary to the Examiner's construction, the claim must be construed to mean that the financial account data is directly retrieved using the biometric data. Because the Examiner appears to have admitted that Pare fails to disclose "direct retrieval of the financial information from the biometric data" (See Office Action at page 4), and because claim 3 *requires* retrieval of the financial information using only the biometric data to identify the financial account, Pare does not disclose the "identifier" of claim 3. Accordingly, even if Pare is modified to include the use of Musgrave's concatenator, the modification does not arrive at invention of claim 3. Thus, under MPEP § 2143.03, the Examiner has failed to present a *prima facie* case of obviousness and the Board of Appeals is respectfully requested to reverse the rejection of claim 3 under 35 U.S.C. 103(a).

4.   Conclusion

For some or all of the above reasons, claim 3 is not obvious in view of the prior art. Accordingly, the Board of Appeals is respectfully requested to reverse this rejection of claim 3.

Discussion Regarding Claim 4

Claim 4 depends from claim 3 and incorporates all of the limitations of claim 3. Therefore, for at least any of the same reasons set forth above with respect to the

rejection of claim 3, the rejection of claim 4 is in error and the Board of Appeals is

respectfully requested to reverse the rejection of claim 4.

Claims 6-7 Are Not Obvious

Discussion Regarding Claim 6

Claim 6 stands rejected under 35 U.S.C. §103(a) as being obvious over

Pare in view of Musgrave. (Office Action at page 5). Claim 6 states:

> A system for verifying access to a consumer's financial account comprising:
> a database server for generating a data storage key from biometric data received from a transaction site; and
> an identity database comprised of data records stored with reference to a data storage key corresponding to biometric data contained within the data record so that the database server may retrieve records from the identity database using data storage keys generated from the received biometric data.

Claim 6 thus recites the use of a biometric data key to retrieve records.

The Examiner rejected claim 6 based upon the same combination of Pare and

Musgrave discussed above with respect to the rejection of claim 1. (Office Action at

page 5). Therefore, the discussion of claim 1 regarding the unavailability of Pare and the

lack of motivation to combine Pare and Musgrave applies to claim 6 and the Board of

Appeals is respectfully requested to reverse this rejection of claim 6.

Discussion Regarding Claim 7

Claim 7 depends from claim 6 and incorporates all of the limitations of claim 6.

Therefore, for at least any of the same reasons set forth above with respect to the

rejection of claim 6, the rejection of claim 7 is in error and the Board of Appeals is

respectfully requested to reverse the rejection of claim 6.

Claim 16 is Not Obvious

Claim 16 stands rejected under 35 U.S.C. §103(a) as being obvious over Pare in view of Musgrave. (Office Action at page 6). The rejection of claim 16 should be reversed.

1.   Claim 16

Claim 16 states:

The method of claim 15, wherein:
the method further comprises,
        obtaining name data corresponding to the consumer, and
        identifying a plurality of data records of a plurality of users based upon
the name data of the consumer; and the step of retrieving comprises,
        retrieving a previously stored data record from the identified plurality
of data records based upon the data storage key.

Claim 16 thus depends from claim 15 and further recites a method of accessing financial data records wherein the data storage key used to identify and retrieve those records is generated using both biometric data and name data from a consumer.

2.   The Discussion of Claim 1 Applies to Claim 16

The Examiner rejected claim 16 based primarily upon the same reasoning set forth above with respect to the rejection of claim 1. (Office Action at page 5). Claim 16 depends from claim 15 and includes all of the limitations of claim 15. Therefore, the discussion of claim 1 which applies to claim 15 further applies to claim 16 and the Board of Appeals is respectfully requested to reverse this rejection of claim 16.

3.   Additional Limitations of Claim 16

Moreover, claim 16 recites that the data storage key is further based upon the name of the consumer. The Examiner alleges that this additional limitation is disclosed in Pare. (Office Action at page 6). The Examiner has failed, however, to identify any portion of Pare which discusses the use of a consumer's name to generate a data storage key. Additionally, the Appellants have searched Pare and found no such teaching, disclosure or suggestion.

Therefore, even if Pare is modified to include the use of Musgrave's concatenator, the modification does not arrive at invention of claim 16. Thus, under MPEP § 2143.03, the Examiner has failed to present a *prima facie* case of obviousness and the rejection of claim 16 under 35 U.S.C. 103(a) should be reversed.

4.   Conclusion

For some or all of the above reasons, claim 16 is not obvious in view of the prior art. Accordingly, the Board of Appeals is respectfully requested to reverse this rejection of claim 16.

Claim 17 is Not Obvious

Claim 17 stands rejected under 35 U.S.C. §103(a) as being obvious over Pare in view of Musgrave. (Office Action at page 5). The rejection of claim 17 should be reversed.

1.   Claim 17

Claim 17 states:

> The method of claim 15, wherein the step of generating comprises:
>> generating a data storage key based upon name data of the consumer.

Claim 17 thus depends from claim 15 and further recites a method of accessing financial data records wherein the data storage key used to identify and retrieve those records is generated using both biometric data and name data from a consumer.

2.   The Discussion of Claim 1 Applies to Claim 17

The Examiner rejected claim 17 based upon the same combination set forth above with respect to the rejection of claim 1. (Office Action at page 5). Claim 17 depends from claim 15 and includes all of the limitations of claim 15. Therefore, the discussion of claim 1 which applies to claim 15 further applies to claim 17 and the Board of Appeals is respectfully requested to reverse this rejection of claim 17.

3.   The Discussion of Claim 16 Applies to Claim 17

The Examiner has failed to identify which prior art teaches, discloses or suggests the limitation added by claim 17. Rather, the Examiner has merely alleged that claim 17 is "unpatentable over [Pare] in view of [Musgrave]. (Office Action at page 5). To the extent the Examiner intended to rely upon Pare for disclosing the limitation of claim 17, Pare has been mischaracterized.

Assuming *arguendo* that the Examiner intended to reject claim 17 relying upon Pare for the limitation added by claim 17, the discussion above with respect to the

rejection of claim 16 applies. Specifically, for purposes of this appeal, the limitation added by claim 17 is analogous to the limitation discussed above that is added by claim 16. Therefore, the discussion of the element added by claim 16 applies to claim 17 and the Board of Appeals is respectfully requested to reverse this rejection of claim 17.

4.   Alternatively, Musgrave Has been Mischaracterized

Alternatively, to the extent the Examiner intended to rely upon Musgrave for the limitation of claim 17, Musgrave has been mischaracterized.

Specifically, claim 17 recites a method of accessing financial data records wherein the data storage key used to identify and retrieve those records is generated using both biometric data and name data from a consumer. The Examiner fails to identify where in Musgrave this additional limitation is disclosed. (Office Action at page 5). Additionally, the Appellants have searched Musgrave and found no such teaching, disclosure or suggestion.

Therefore, even if Pare is modified to include the use of Musgrave's concatenator, the modification does not arrive at invention of claim 17. Thus, under MPEP § 2143.03, the Examiner has failed to present a *prima facie* case of obviousness and the rejection of claim 17 under 35 U.S.C. 103(a) should be reversed.

5.   Conclusion

For some or all of the above reasons, claim 17 is not obvious in view of the prior art. Accordingly, the Board of Appeals is respectfully requested to reverse this rejection of claim 17.

26

(8) CONCLUSION

Claims 1-4, 6-11 and 13-17 are not obvious over Pare in view of Musgrave.

Accordingly, the Board of Appeals is respectfully requested to reverse the rejections of

claims 1-4, 6-11 and 13-17.

Respectfully submitted,

MAGINOT, MOORE & BECK

James D. Wood
Attorney for Appellants
Registration No. 43,285

January 11, 2006
Maginot, Moore & Beck
Chase Tower
111 Monument Circle, Suite 3250
Indianapolis, Indiana 46204-5115
Telephone (317) 638-2922

(9) CLAIMS APPENDIX

Claim 1.   A system for providing consumer access to a financial account to implement a transaction comprising:

a biometric data capture device for reading consumer biometric data; and

a database server for generating a data storage key from the consumer biometric data received from the biometric data capture device and for retrieving a financial account data record corresponding to the generated data storage key.

Claim 2.   The system of claim 1 further comprising:

a payment device coupled to said biometric data capture device, said payment device generating a digital signature from said biometric data for a transaction message.

Claim 3.   A system for supporting consumer access to a financial account by means of biometric data solely, the system comprising:

a biometric data capture device for capturing biometric data corresponding to a consumer; and

a payment device for sending said captured biometric data to a merchant payment host as the identifier for the consumer's financial account data.

Claim 4.   The system of claim 3, wherein said payment device generates a digital signature from said captured biometric data.

Claim 6.   A system for verifying access to a consumer's financial account comprising:

a database server for generating a data storage key from biometric data received from a transaction site; and

an identity database comprised of data records stored with reference to a data storage key corresponding to biometric data contained within the data record so that the database server may retrieve records from the identity database using data storage keys generated from the received biometric data.

Claim 7.   The system of claim 6 wherein the database server generates a digital signature from biometric data retrieved from the identity database so that a transaction message may be verified.

Claim 8.   A method for accessing a financial account for a consumer comprising:

generating a data storage key from biometric data corresponding to a consumer; and

retrieving a data record stored in a memory using the generated data storage key, the data record corresponding to the generated data storage key and containing financial account data for the consumer.

Claim 9.   The method of claim 8 further comprising generating a digital signature from the biometric data corresponding to the consumer to authorize generation of electronic funds transfer messages for a financial transaction.

Claim 10.   The method of claim 8 further comprising:

capturing the biometric data corresponding to the consumer; and

transmitting the captured biometric data so the data storage key may be generated.

Claim 11.   The method of claim 9 further comprising comparing the generated digital signature to a received digital signature to authorize generation of electronic funds in response to said generated digital signature corresponding to said received digital signature.

Claim 13.   A method for accessing a financial account of a consumer comprising:

capturing biometric data corresponding to a consumer;

sending the captured biometric data to a merchant payment host to obtain financial account data from the merchant payment host; and

retrieving a financial record identified at least in part by previously captured biometric data, wherein the captured biometric data is used to retrieve the financial record.

Claim 14.   The method of claim 13 further comprising:

generating a digital signature from the captured biometric data; and

transmitting the generated signature in a transaction message to the merchant payment host for authorizing generation of electronic transfer messages by the merchant payment host.

Claim 15.   A method of accessing financial data records comprising:

capturing biometric data corresponding to a consumer;

generating a data storage key based upon the captured biometric data; and

retrieving a previously stored data record based upon the data storage key.

Claim 16.   The method of claim 15, wherein:

the method further comprises,

obtaining name data corresponding to the consumer, and

identifying a plurality of data records of a plurality of users based upon the name data of the consumer; and the step of retrieving comprises,

retrieving a previously stored data record from the identified plurality of data records based upon the data storage key.

Claim 17.   The method of claim 15, wherein the step of generating comprises:

generating a data storage key based upon name data of the consumer.

(10) EVIDENCE APPENDIX

None.

(11) RELATED PROCEEDINGS APPENDIX

None.